Manual de Usuario de Bellator

1. INTRODUCCIÓN.

Bellator es un programa para la auditoría de sistemas en función de unas plantillas predeterminadas de seguridad.

Por lo tanto el objeto de *Bellator* es comprobar si están aplicados los parámetros de dichas plantillas y revisar el estado su implantación.

Se puede utilizar *Bellator* para auditar un sistema después de la aplicación de la configuración de seguridad sobre el mismo o de forma periódica para saber el nivel de cumplimiento de la configuración segura y conocer si ha habido cambios, no declarados, sobre el sistema.

Las plantillas que utiliza son de dos tipos:

- Política Local de Seguridad, cuya extensión es INF.
- Plantillas Administrativas de Seguridad (dentro de la Directiva de Equipo Local, tanto la configuración del Equipo como la configuración de Usuario). Extensión POL.

La plantilla de la Política Local de Seguridad se puede obtener de dos formas:

- A través de Microsoft, gracias a sus guías de configuración segura, se pueden descargar las plantillas (INF) que se quiera comprobar.
- Exportándolas de un sistema previamente configurado de forma segura (Secedit /export /cfg [nombre_del_fichero.inf]), de esta forma se podría comprobar de forma periódica cualquier cambio en la configuración inicial.

Las Plantillas Administrativas de Seguridad se podrán obtener de la carpeta Group Policy de un sistema configurado de forma segura.

Además de la información relativa a las plantillas expuestas con anterioridad, el programa presenta otra serie de datos de interés, como son, usuarios, grupos, sistema operativo, Service Pack, particiones, tamaño del disco y espacio libre y memoria RAM.

2. MANUAL DE USO

a. Requisitos

Para que *Bellator* funcione correctamente requiere la herramienta de Microsoft, SubInACL.exe (http://www.microsoft.com/downloads/details.aspx?FamilyID=E8BA3E56-D8FE-4A91-93CF-ED6985E3927B&displaylang=en) para la obtención de permisos en el lenguaje SDDL (Security Descriptor Definition Language http://msdn.microsoft.com/en-us/library/aa379567(VS.85).aspx) de ficheros, servicios, claves de registro, etc.

También es imprescindible que esté en el sistema, la librería msvcr70.dll que es un módulo que contiene funciones de biblioteca estándar de C.

Ambos ficheros se proporcionan están integrados en el ejecutable *Bellator*. Si no fuese así, deberían estar en la misma carpeta.

Como entrada se requieren las plantillas (INF y POL) que se han descrito anteriormente. Es fundamenta renombrar los ficheros como:

- **template.inf**. Correspondiente a la plantilla de la Política Local de Seguridad.
- **RegistryM.pol** y **RegistryU.pol** según corresponda a las plantillas administrativas de configuración del equipo o de usuario.

En la última versión se ha procedido a proporcionar varias opciones, que serán pasadas por línea de comandos. A saber.

Especificación de las ubicaciones de las plantillas:

- *-T [Fichero.inf]*
- *–GU [registry.pol de Usuario]*
- *–GM [Registry.pol de Máquina]*

En caso contrario buscará los ficheros con los nombre por defecto del programa (template.inf, RegistryU.pol y RegistryM.pol).

Los informes pueden ser enviados vía FTP a un servidor, utilizando las siguientes opciones:

- *-F [IP_Servidor_FTP]*
- *-U [Usuario_FTP]*
- *-P [Password_FTP]*

Como el programa necesita guardar (escribir) sobra la carpeta donde va a copiar los informes, requiere los permisos necesarios de escritura para el usuario proporcionado.

También puede enviar los informes a un recurso compartido. Esta opción es válida para equipos en dominio, porque la autenticación es transparente para el programa:

- *-S [IP_Servidor]*
- *-R [Recurso_Compartido]*

Si se desea un modo similar a "silencioso" o "quiet", donde no aparezcan mensajes y no sea necesaria la intervención del usuario, existe la opción:

- *-NM*

Además, si se desea obtener un informe más detallado (AllResult.txt), si no se obtendrá el informe de resultados únicamente:

- *-D*

Se puede extender el formato de los nombres de los informes, para realizar varios análisis en un mismo día, añadiendo al nombre, la hora de de realización de la auditoría:

- *-E*

Se ha añadido un chequeo de parches (hotfix) de Microsoft. Para ello se necesita un fichero como plantilla (con los KBs de los productos Microsoft) y activar la opción

- *-HF [Fichero_Hotfix]*

Y como no, una opción de ayuda:

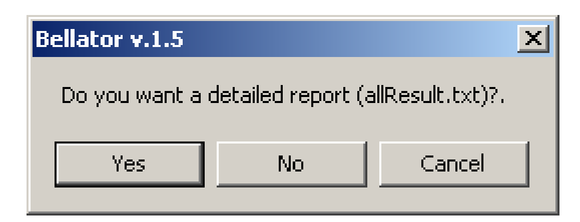
- *-H*

Por último, comentar que *Bellator* ha sido testado en clientes independientes y clientes de dominio en sistemas Windows 2000 Server/Professional (inglés y español) y Windows XP Professional (inglés y español) y Windows 2003 (inglés y español).

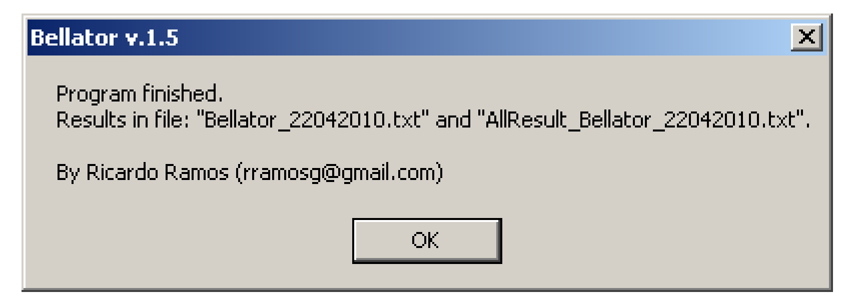
b. Ejecución

Llegados a este punto, sólo falta ejecutar *bellator.exe*.

Bellator preguntará si se desea obtener un informe con el detalle de los datos obtenidos, además del informe de resultados que se proporciona en cualquier caso.



Bellator notifica al usuario de la finalización correcta del programa, así como la denominación de los informes (que corresponderá al nombre de máquina y la fecha de la ejecución).



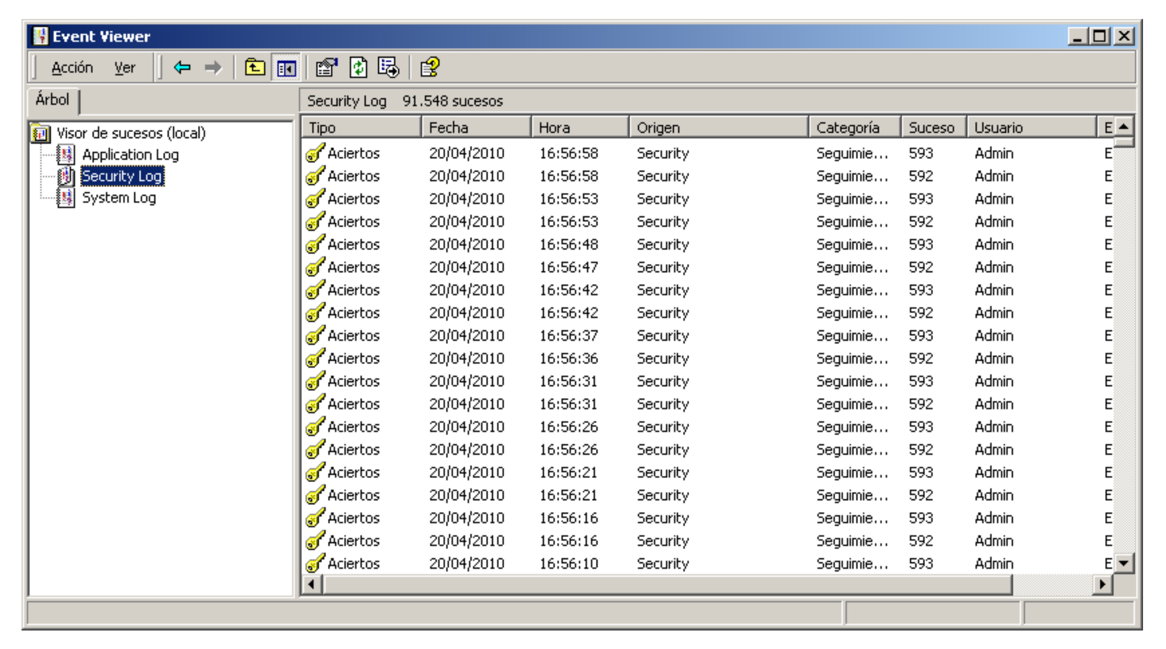
c. Estructura plantillas Directivas Locales de Seguridad

La plantilla de seguridad debe tener un formato determinado, agrupando cada módulo de auditoría por unas determinadas etiquetas (ej. [Application Log]):

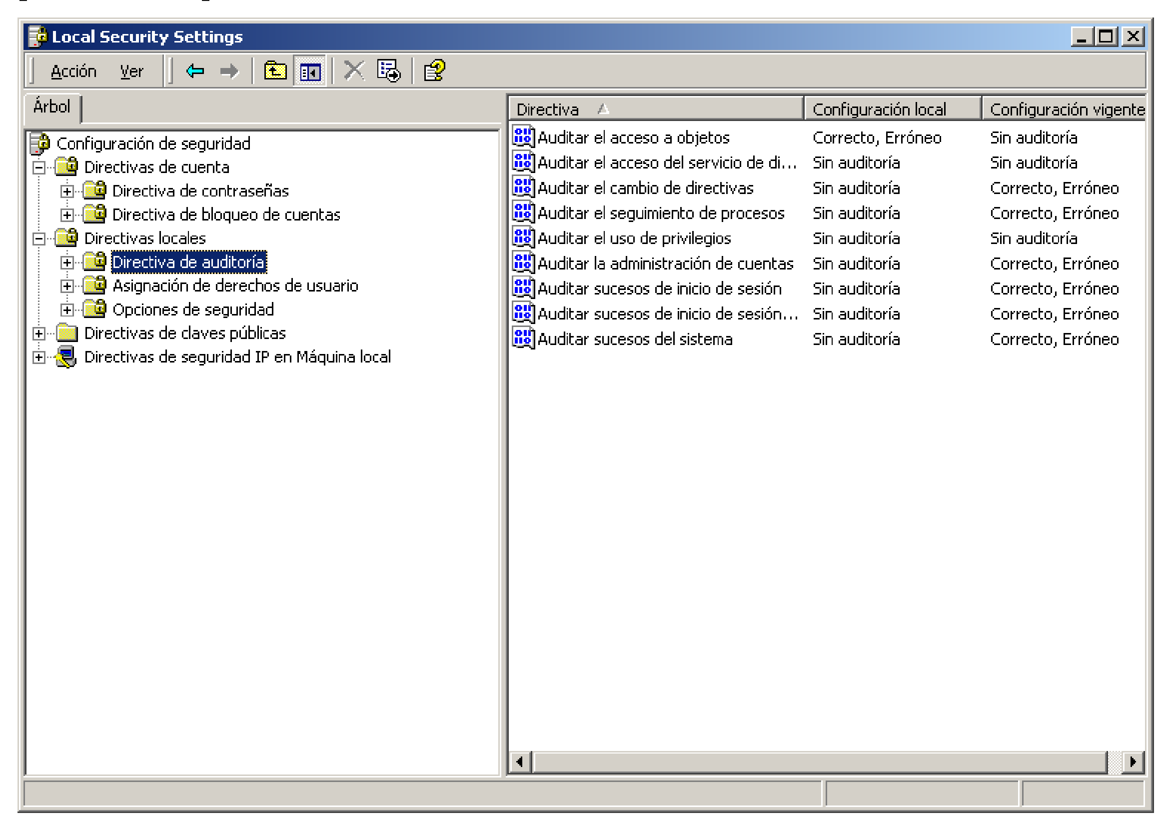
```
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 2
AuditPolicyChange = 1
[Service General Setting]
Alerter,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCLCSWLOCRRC;;;AU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
CiSvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCLCSWLOCRRC;;;AU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```

Se enumeran a continuación:

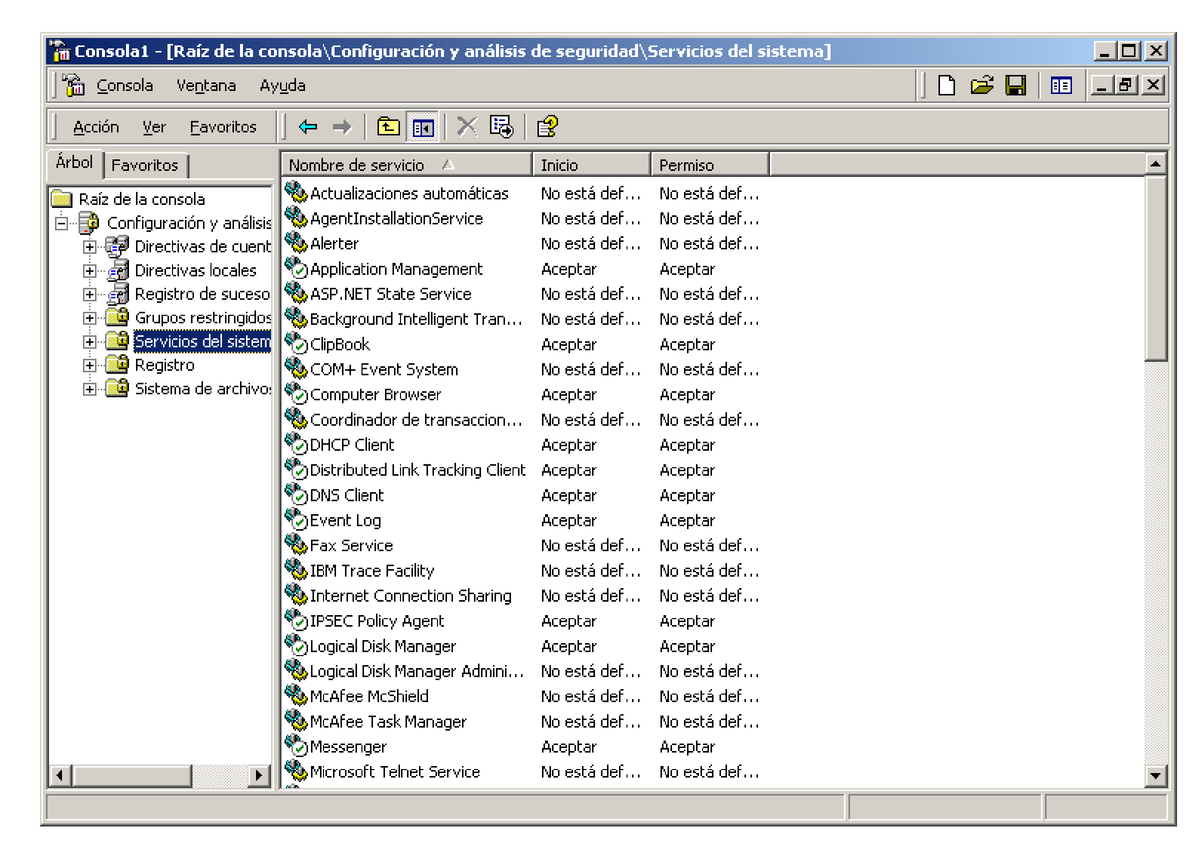
- [System Log], [Security Log], [Application Log]: Evento del sistema, seguridad y aplicación (Visor de sucesos).



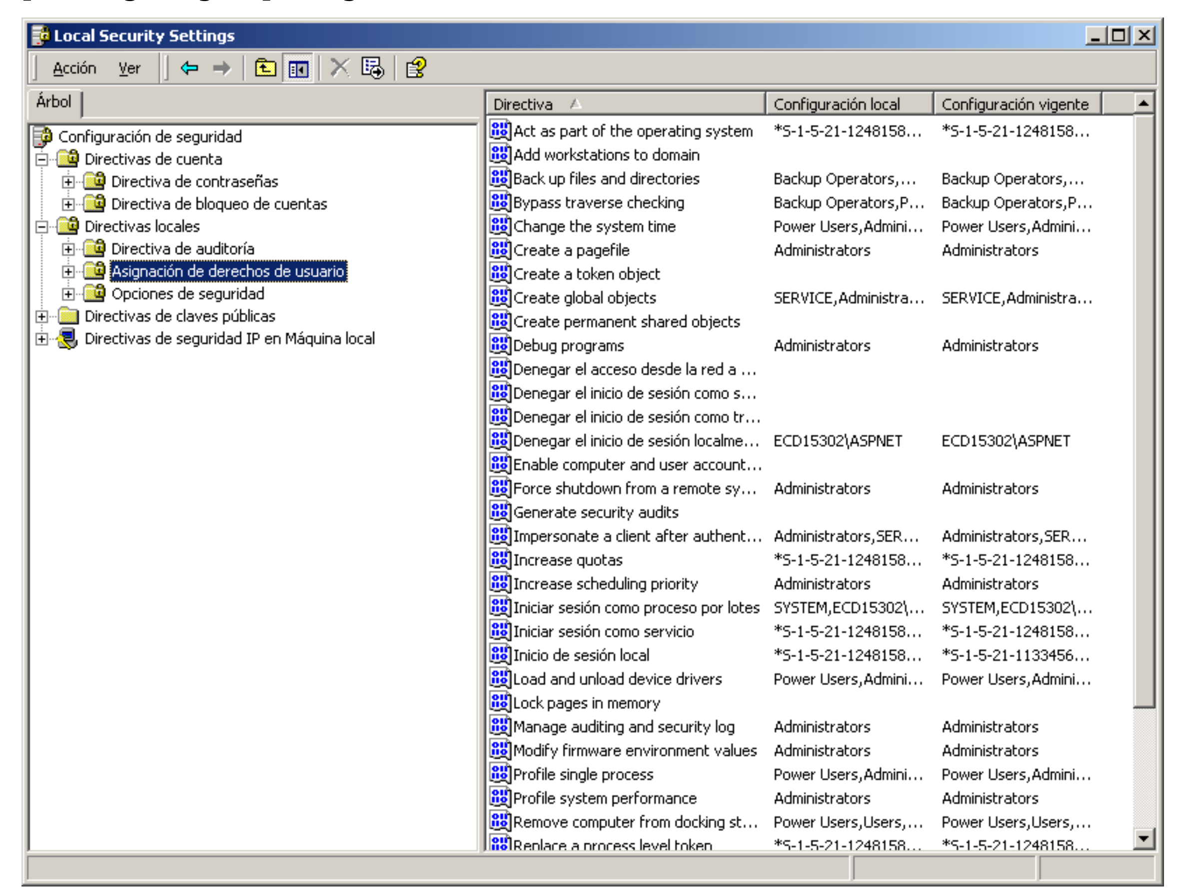
- [Event Audit]: Directiva de auditoría



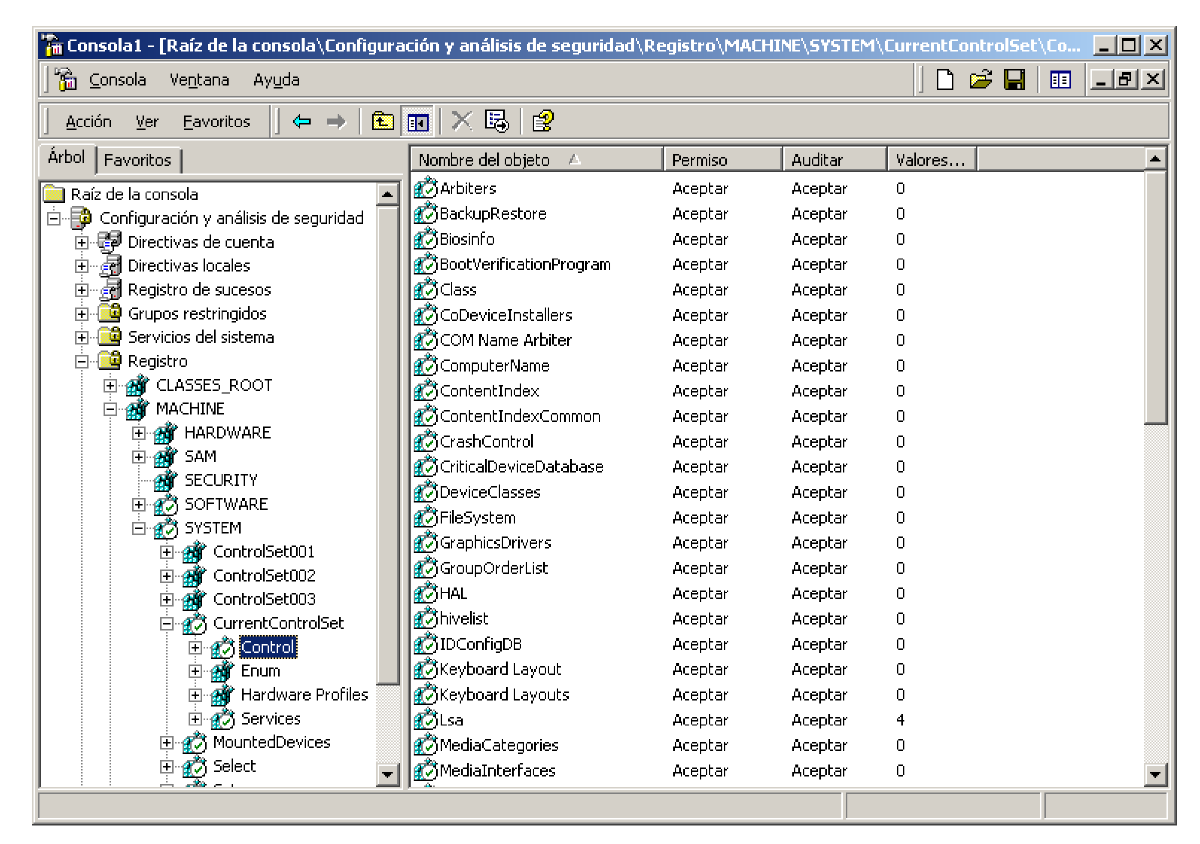
- [Service General Setting]: Permisos sobre servicios del sistema



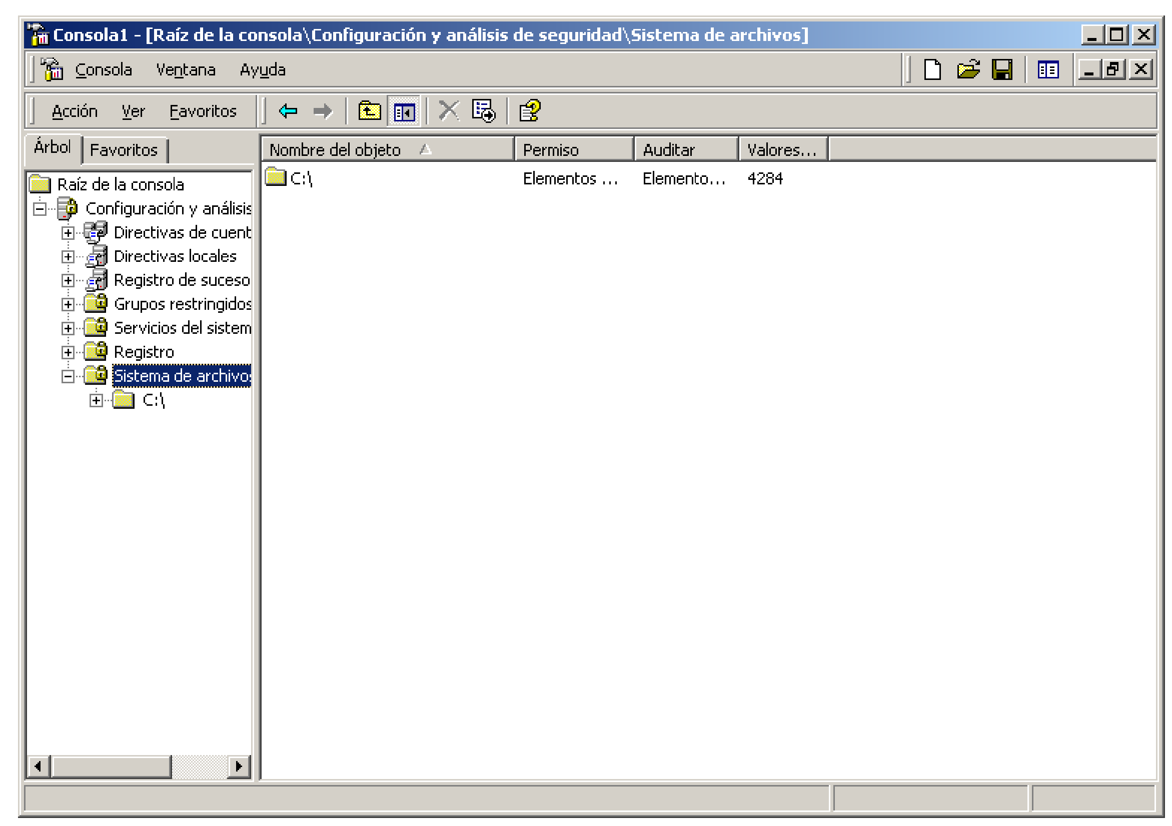
- [Privilege Rights]: Asignación de derechos de usuario



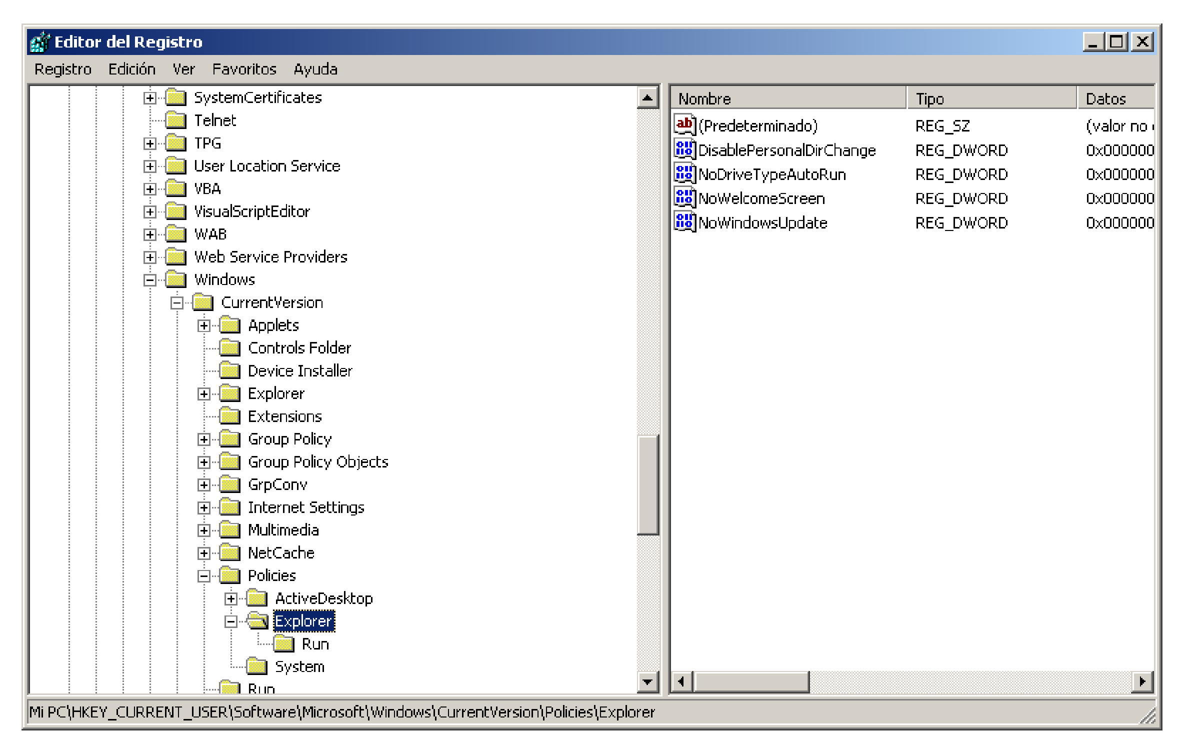
- [Registry Keys]: Permisos sobre claves del registro del sistema



- [File Security]: Permisos sobre ficheros del sistema



- [Registry Values]: Valores de claves del registro del sistema. Cubre diferentes parte de la guía de configuración, entre otros lo relativo a Opciones de Seguridad.



Bellator no cubre lo relativo a Directivas de Cuentas [System Access], que se tendrá que hacer manualmente por el momento.

Bellator se puede ejecutar, también, a través de las opciones presentadas en el punto anterior.

```
C:\WINDOWS\system32\cmd.exe
C:\>bellator.exe -h

####################################################
#####    Ricardo Ramos (rramosg@gmail.com)    #####
####################################################

usage: bellator [-T] [-GU] [-GM] [-F(-U|-P)] [-S(-R)] [-E] [-NM(-D)] [-help|-?]
-T:     Policy INF file
-GU:    Local Computer Policy relative to user configuration
-GM:    Local Computer Policy relative to machine configuration
-F:     IP Address of the FTP Server. To send reports by means of FTP Service
        -U:FTP Service user. User must have write permission on folder
        -P:FTP Service password
-S:     IP Address of the Server (Resource Shared). Active Directory option, bec
ause does not need login in the Domain Controller
        -R:Shared folder in the Server (Active Directory). User must have write
permission on folder
-E:     Extend name of the file. Add time to the name od the report (ex. server_
10112010_140530.txt)
-NM:    Execute the program without interaction with the user. Not appear messag
es
        -D:Permit get the report with more detail (ex. Allresult_server_10112010
.txt)
-H:     Show the Help
```

Ejemplo de comando:

```
C:\WINDOWS\system32\cmd.exe

C:\>bellator.exe -T "C:\Bellator\WinXP_Security.inf" -GU "C:\Bellator\GroupPolic
y\User\Registry.pol" -GM "C:\Bellator\GroupPolicy\Machine\Registry.pol" -E -NM -
D -F 10.128.41.95 -U audit -P securityPass_
```

Además, se puede ejecutar a través del Programador de Tareas de Windows, trabajos programados con la frecuencia que se considere y enviar los report donde se requieran y así facilitar la tarea de control de la seguridad sobre los sistemas.

d. Estructura de las Plantillas Administrativas de Seguridad

Los ficheros RegistryM.pol y RegistryU.pol, deben cumplir el formato ABNF (http://download.microsoft.com/download/9/5/E/95EF66AF-9026-4BB0-A41D-A4F81802D92C/%5BMS-GPREG%5D.pdf). No debe ser modificado con un editor de texto al uso puesto que está en hexadecimal y puede introducir caracteres erróneos.

e. Resultados

Los resultados presentan las siguientes posibilidades:

- En caso de coincidir el resultado sería positivo y por tanto no aparece en el informe de resultados.
- En caso de no coincidir se muestra en el informe y se consideran, en función del motivo de la divergencia, de dos formas diferentes:
  - Considerarse como resultado negativo y por tanto se catalogaría como resultado "INCORRECT", "ERROR" o "… does not coincide".
  - Considerarse como resultado positivo pero con alguna modificación menor, a nuestro juicio, que no afecta a la seguridad del parámetro/equipo. Se presenta como "CORRECT but…"
    - Ejemplo: "CORRECT PERMISSION although some flags do not match with "C:\Program Files\Windows Media Player""

      En este caso, la plantilla especifica los siguientes permisos: "D:PAR(A;**OICI**;FA;;;BA)(A;**OICI**;0x1200a9;;;BU)(A;**OICI**;FA;;;SY)"

      Y en la máquina: D:PAR(A;;FA;;;BA)(A;;0x1200a9;;;BU)(A;;FA;;;SY)

Como se puede apreciar, no coincide el ACE flag que hace referencia a la herencia del fichero.

Por tanto, se avisa de que hay algo incorrecto aunque según nuestro criterio, los suficientemente laxo como para darlo por correcto. En cualquier caso, se notifica, precisamente para dejar en manos del usuario la decisión final.

- Por último, se puede presentar un resultado con advertencia de que se debe realizar una comprobación manual del parámetro. Es debido a que en raras ocasiones, los valores no son tratados correctamente.

f. Descarga

Se puede descargar en:

- http://code.google.com/p/bellator/downloads/list
- http://sourceforge.net/projects/bellator/files/

3. COLABORACIONES

Bellator es un proyecto iniciado hace tiempo y resultado del esfuerzo de su autor pero en el cual, han contribuido en diversas facetas, personas a la cuales quiero agradecer su apoyo altruista al proyecto.

Ellos son:

Manuel Rodríguez. El cual se ha encargado de coordinar las pruebas de *Bellator* sobre diversos sistemas y en diversos entornos para la depuración de errores.

Serg por sus aportaciones y representación "comercial" de *Bellator*.

Yago por su inestimable ayuda, sobre todo a la hora de comenzar a lidiar con éste morlaco que es la programación en Windows.

Y algún que otro compañero/amigo/colega por la aportación de sus ideas y algo más ;).

4. CONTACTO

Para cualquier sugerencia, error, crítica (constructiva) o simplemente consulta sobre *Bellator*, se pueden dirigir a bellator.audit@gmail.com.

Muchas gracias.

Ricardo.